A Secured Approach to Visual Cryptographic Biometric Template

Rahna. P. Muhammed
M.Tech Student, Dept of CSE
Viswajyothi College of Engineering and Technology
Vazhakkulam, Muvattupuzha
rahnap2000@gmail.com

***Abstract*— BIOMETRIC authentication systems are gaining wide-spread popularity in recent years due to the advances in sensor technologies as well as improvements in the matching algorithms. Most biometric systems assume that the template in the system is secure due to human supervision (e.g., immigration checks and criminal database search) or physical protection (e.g., laptop locks and door locks). Preserving the privacy of digital biometric data (e.g., face images) stored in a central database has become of paramount importance. VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. This work improves the security of visual cryptography by scrambling the image using random permutation.**

***Index Terms*— Visual cryptography, Image scrambling, Random permutation**

I. Introduction

BIOMETRICS is the science of establishing the identity of an individual based on physical or behavioral traits such as face, fingerprints, iris, etc. The working of biometric authentication system is by acquiring raw biometric data from a subject, extracting a feature set from the data, and comparing the feature set against the templates stored in a database in order to identify the subject or to verify a claimed identity. The biometric template is generated during enrollment and is stored in the database. For protecting the privacy of an individual enrolled in a biometric database, Davida *et al.* [1] and Ratha *et al.* [2] proposed storing a transformed biometric template instead of the original biometric template in the database. Apart from these methods, various image hiding approaches [3]–[5] have been suggested by researchers to provide anonymity to the stored biometric data. In this paper to enhance the security of the template, a system is proposed by applying scrambling to the image and apply the visual cryptography. This paper is organized as follow: visual cryptographic scheme is discussed in section 2, details of random permutation is discussed in section 3, section 4 presents the proposed system.

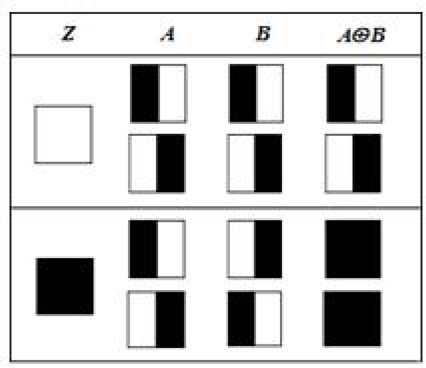
II. Visual Cryptography

Cryptography is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Naor and Shamir [6] introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations. This scheme is referred to as the *k*-out-of-*n* VCS which is denoted as (*k*,*n*)VCS. Given an original binary image, it is encrypted in *n* images, such that

$$T = S_{h1} \oplus S_{h2} \oplus S_{h3} \oplus \ldots\ldots\ldots\ldots S_{hn} \qquad (1)$$

where Å is a Boolean operation, S_{hi}, h_i Î 1,2,….*k* is an image which appears as white noise, *k* d" *n*, and *n* is the number of noisy images. It is difficult to decipher the secret image *T* using individuals S_{hi}'s [6]. The encryption is undertaken in such a way that *k* or more out of the *n* generated images are necessary for reconstructing the original image *T* . In the case of (2, 2) VCS, each pixel *P* in the original image is encrypted into two sub pixels called shares. For biometric privacy, here 2-out-of-2 scheme is using.

TABLE I
Encoding a binary pixel *P* into 2 shares A and B



In this scheme for sharing a single pixel p, in a binary image Z into two shares A and B is illustrated in Table I. If p is white, one of the first two rows of Table 1 is chosen randomly to encode A and B. If p is black, one of the last two rows in Table 1 is chosen randomly to encode A and B. Thus, neither A nor B exposes any clue about the binary color of p. When these two shares are superimposed together, two black sub-pixels appear if p is black, while one black sub-pixel and one white sub-pixel appear if p is white as indicated in the rightmost column in Table 1. Based upon the contrast between two kinds of reconstructed pixels can tell whether p is black or white.

DOI: 01.IJNS.02.03.161

III. Scrambling Through Random Permutation

A random permutation is a permutation containing a fixed number ***n*** of a random selection from a given set of elements. The *plain image* can be decomposed into blocks; each one contains a specific number of pixels (4 pixels × 4 pixels blocks). Increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy. The blocks are transformed into new locations. The permutation process refers to the operation of dividing and replacing an arrangement of the original image, and thus the generated one can be viewed as an arrangement of blocks [7],[8]. The block diagram of permutation scheme is shown in Fig 1.

A. *Algorithm Perform_Permutation*

Input: plain image (BMP image file) and permutation table
Output: permuted image.

1. Load the plain Image
2. Input secret key
3. Get the Width and Height of the image
4.

4.1. Lower Horizontal Number of Blocks = Integer (Image Width / 4)
4.2. Lower Vertical Number of Blocks = Integer (Image Height /4)

5. Number of Blocks = Horizontal Number of Blocks × Vertical Number of Blocks
6. Seed = | Hash value (Key) |
7. Randomize ()
8. For I = 0 to Number of Blocks -1

8.1 Get the new location of block I from the permutation table
8.2 Set block I in its new location

9. End perform_permutation

IV. Proposed System

Protecting template in the database securely is one of the challenges in any biometric system. Here visual cryptography is applied to biometric authentication system [9]. In this system, there are two modules: *Enrollment module* and *Authentication module*.

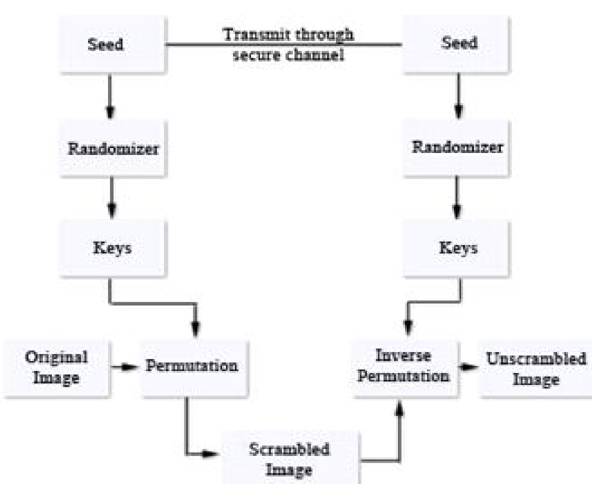


Fig. 1. Block diagram of permutation scheme.

A. *Enrollment module :*

During the enrollment process, administrator collects the template and performs image scrambling. Image scrambling is used to make images visually unrecognizable such that unauthorized users have difficulty decoding the scrambled image to access the original image. Image scrambling is done by applying the above permutation algorithm. Using the key value some permuted sequence will be generated and apply the sequence to the image. The original image can be decomposed into blocks; each one containing a specific number of pixels. The blocks are transformed into new locations by the above permuted sequence, which produces the scrambled image. The scrambled image is then sent to a trusted third-party entity. Once the trusted entity receives it, the scrambled image is decomposed into two noisy images (i.e., sheets) and the original data is discarded. The decomposed components are then transmitted and stored in two different database servers such that the identity of the private data is not revealed to either server.

B. *Authentication module :*

During the authentication process, the trusted entity sends a request to each server and the corresponding sheets are transmitted to it. Sheets are overlaid (i.e., superimposed) in order to reconstruct the scrambled image. An inverse permutation sequence is obtained by using the same key, and applies this sequence to the scrambled image in-order to reconstruct the original image.

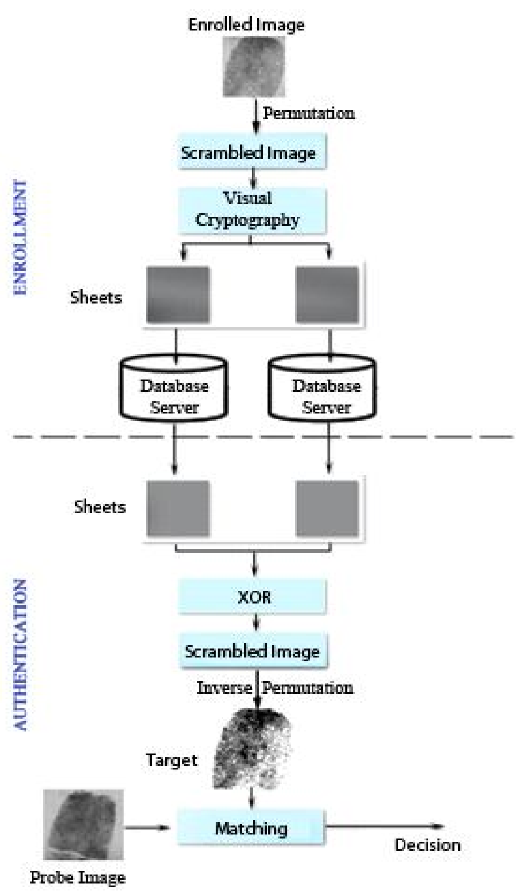


Fig 2. Proposed approach for de-identifying and storing a finger print image

DOI: 01.IJNS.02.03.161

The use of basic visual cryptography for securing fingerprint iris and face templates was suggested in [10] , [11] and [12] respectively. By using the proposed method, as shown in Fig. 2, the biometric template is scrambled and decomposed by the visual cryptography scheme and two noise-like images known as sheets are produced. For faces each private face image is scrambled and decomposed into two independent public host images. The public images hosting the private face images are referred to as sheets.

V. Conclusions

This paper explored the security of visual cryptography by scrambling the image using random permutation. Here, the templates are scrambled and decomposed into two noise-like images using (2,2) VCS, and since the spatial arrangement of the pixels in these images varies from block to block, it is impossible to recover the scrambled image without accessing both the shares and an XOR operator is used to superimpose the two noisy images to get the scrambled image. Hence this paper contributes a more secured approach to biometric data privacy.

REFERENCES

[1]. G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in *Proc. IEEE Symp. Security and Privacy*, 1998, pp. 148–157.

[2]. N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.

[3]. Jain and U. Uludag, "Hiding biometric data," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 11, pp. 1494–1498, Nov. 2003.

[4]. J. Dong and T. Tan, "Effects of watermarking on iris recognition performance," in *Proc. 10th Int. Conf. Control, Automation, Robotics and Vision, 2008 (ICARCV 2008)*, 2008, pp. 1156–1161.

[5]. N. Agrawal and M. Savvides, "Biometric data hiding: A 3 factor authentication approach to verify identity with a single image using steganography, encryption and matching," in *Proc. Computer Vision and Pattern Recognition Workshop*, 2009, vol. 0, pp. 85–92.

[6]. M.Naor and A. Shamir, "Visual cryptography," in *Proc. EUROCRYPT*, 1994, pp. 1–12.

[7]. Mitra, Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, vol.1, no. 1, 2006, p.127, http://www.enformatika.org.

[8]. Mohammad Ali Bani Younes and Aman Jantan "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.4, April 2008

[9]. A.Ross and A.A.Othman,"Visual cryptography for biometric privacy",IEEE transactions on information forensics and security,Vol.6,No.1,March 2011.

[10]. Y. Rao, Y. Sukonkina, C. Bhagwati, and U. Singh, "Fingerprint based authentication application using visual cryptography methods (improved id card)," in *Proc. IEEE Region 10 Conf.*, Nov. 2008, pp.1–5.

[11]. P.Revenker, A. Anjum, and W. Gandhare, "Secure iris authentication using visual cryptography," *Int. J. Comput. Sci. (IJCSIS)*, vol. 7, no. 3, pp. 217–221, Mar. 2010.

[12]. A. Ross and A. A. Othman, "Visual cryptography for face privacy," in *Proc. SPIE Biometric Technology for Human Identification VII*, Orlando,FL, 2010, vol. 7667.

DOI: 01.IJNS.02.03.161